OTP vis SMS Integration

This document describes the design and implementation of the OTP (One-Time Password) via SMS system for secure internal transfers, using the **Semaphore SMS Gateway**. The system is implemented in PHP and is designed to enhance security for sensitive transactions between users.

Workflow Overview

1. The user initiates a transfer.
2. The backend (transfer_otp_generate.php) generates a random OTP, stores it (with expiry), and sends it to the user's registered mobile number via the Semaphore API.
3. The user receives the OTP via SMS and enters it in the frontend.
4. The backend (verify_transfer_otp.php) verifies the OTP. If valid and not expired, the transfer is completed.
5. On successful OTP verification, the system updates account balances and logs the transaction.

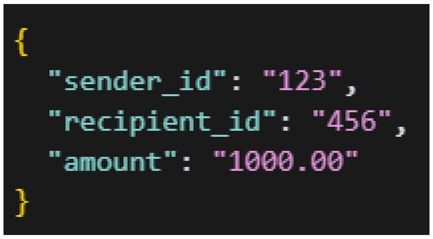
API Endpoints

1. **Generate OTP for Transfer**

Endpoint: POST /transfer_otp_generate.php

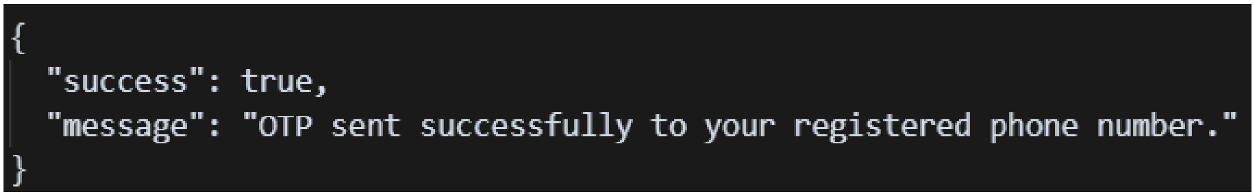
Description: Generates and sends an OTP to the sender's registered mobile number for a transfer.

Input (JSON):



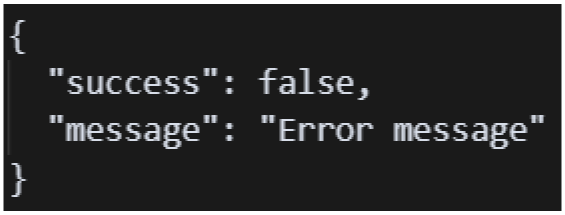
```
{
  "sender_id": "123",
  "recipient_id": "456",
  "amount": "1000.00"
}
```

Response (JSON): On success



```
{
  "success": true,
  "message": "OTP sent successfully to your registered phone number."
}
```

Response (JSON): On failure



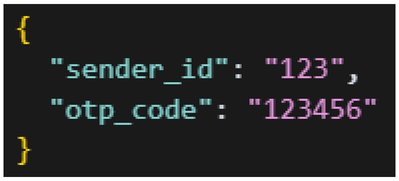
```
{
  "success": false,
  "message": "Error message"
}
```

2. Verify OTP and Complete Transfer

Endpoint: POST /verify_transfer_otp.php

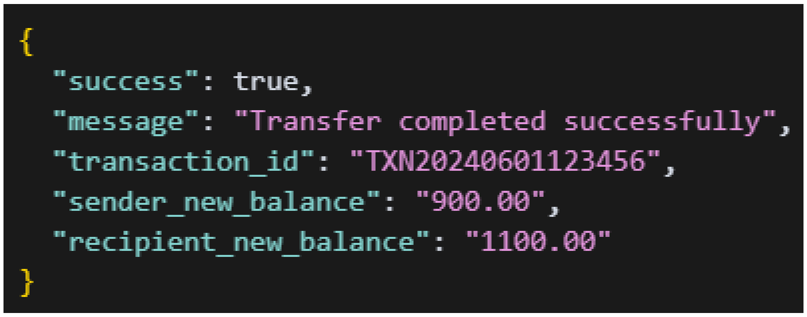
Description: Verifies the OTP entered by the user and, if valid, completes the transfer.

Input (JSON):



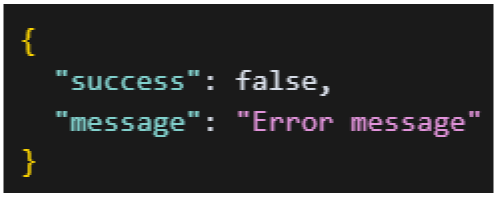
```
{
  "sender_id": "123",
  "otp_code": "123456"
}
```

Response (JSON): On success



```
{
  "success": true,
  "message": "Transfer completed successfully",
  "transaction_id": "TXN20240601123456",
  "sender_new_balance": "900.00",
  "recipient_new_balance": "1100.00"
}
```

Response (JSON): On failure



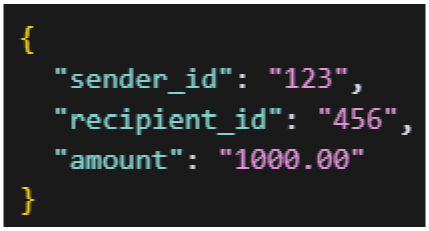
```
{
  "success": false,
  "message": "Error message"
}
```

3. Internal Transfer (Session-based, after OTP)

Endpoint: POST /transfer_internal.php

Description: Performs the actual transfer between accounts. This is called after OTP verification, using session authentication.

Input (JSON):



```
{
  "sender_id": "123",
  "recipient_id": "456",
  "amount": "1000.00"
}
```

Response: Standard JSON indicating success or failure, with updated balances.

Security Considerations

- OTPs expire after 5 minutes.
- OTPs are deleted after successful use or expiry.
- Logging of invalid attempts is implemented.
- Checks for valid session and sender identity.
- OTPs are stored in plain text in JSON files for simplicity.

Testing Checklist

- OTP is sent successfully to valid mobile numbers.
- OTP is saved and expires correctly.
- Verification fails after OTP expires.
- OTP cannot be reused.
- Transfer only proceeds after successful OTP verification.
- All actions are logged for audit and debugging.